UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	35.G2331
First Named Inventor or Application Identifier	KAZUOMI OISHI
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [ ] Fee Transmittal Form *(Submit an original, and a duplicate for fee processing)*
2. [X] Specification — *Total Pages* 37
3. [X] Drawing(s) *(35 USC 113)* — *Total Sheets* 5
4. [X] Oath or Declaration — *Total Pages* 1
   - a. [ ] Newly executed (original or copy)
   - b. [X] Unexecuted for information purposes
   - c. [ ] Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 17 completed)* ***[Note Box 5 below]***
     - i. [ ] DELETION OF INVENTOR(S) Signed Statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. [ ] Incorporation By Reference *(useable if Box 4c is checked)* The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4c, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. [ ] Microfiche Computer Program *(Appendix)*
7. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   - a. [ ] Computer Readable Copy
   - b. [ ] Paper Copy (identical to computer copy)
   - c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. [ ] Assignment Papers (cover sheet & document(s))
9. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [ ] Power of Attorney
10. [ ] English Translation Document *(if applicable)*
11. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
12. [ ] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
14. [ ] Small Entity Statement(s) [ ] Statement filed in prior application Status still proper and desired
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Other: _____

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information:*
    [ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No. ___/_____

18. CORRESPONDENCE ADDRESS

[X] Customer Number or Bar Code Label — 05514 (Insert Customer No or Attach bar code label here) — or [ ] Correspondence address below

NAME					
Address					
City		State		Zip Code	
Country		Telephone		Fax	

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS (37 CFR 1.16(c))	22-20 =	2	X $ 18.00 =	$ 36.00
	INDEPENDENT CLAIMS (37 cfr 1.16(b))	10-3 =	7	X $ 78.00 =	$ 546.00
	MULTIPLE DEPENDENT CLAIMS (if applicable) (37 CFR 1.16(d))			$260.00 =	$ 0.00
				BASIC FEE (37 CFR 1.16(a))	$ 760.00
			Total of above Calculations =		$1,342.00
	Reduction by 50% for filing by small entity (Note 37 CFR 1.9, 1.27, 1.28).				
				TOTAL =	$1,342.00

19. Small entity status

a. ☐ A Small entity statement is enclosed

b. ☐ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.

c. ☐ Is no longer claimed.

20. ☒ A check in the amount of $ 1,342.00 to cover the filing fee is enclosed.

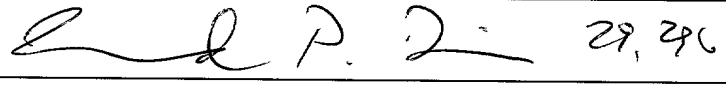
21. ☐ A check in the amount of $ _____ to cover the recordal fee is enclosed.

22. The Commissioner is hereby authorized to credit overpayments or charge the following fees to Deposit Account No. 06-1205:

a. ☒ Fees required under 37 CFR 1.16.

b. ☒ Fees required under 37 CFR 1.17.

c. ☐ Fees required under 37 CFR 1.18.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED	
NAME	Leonard P. Diana
SIGNATURE	
DATE	December 29, 1998

F502\A628217\mfg

TITLE OF THE INVENTION

IMAGE INPUT APPARATUS, IMAGE INPUT METHOD, RECORDING MEDIUM, AND ENCRYPTION PROCESSING PROGRAM STORED IN COMPUTER-READABLE MEDIUM

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to an image input apparatus, an image input method, a recording medium, and an encryption processing program stored in a computer-readable medium. More particularly, the invention relates to a technique for protecting the copyright for image signals.

Description of the Related Art

In image input apparatuses, such as still cameras, video cameras, and scanners, all of which are of the analog type, analog image signals, such as motion pictures or still images, obtained by photographing subjects, are converted into recordable/reproducible signals, which are then output to an external source. Alternatively, such analog image signals are recorded on a recording medium by using a recording apparatus.

Generally, since the data in the above-described

recording medium can be stored over a long period, it is suitable to observe or reuse the stored analog image information later. Accordingly, in response to the user's demand, a reproducing apparatus reads analog image information recorded on the recording medium and reconstitutes it to an image that can be viewed by humans. The image is then reproduced through an output apparatus, such as a printer or a display unit.

Because of recent progress in digital technology, analog-type image input apparatuses are gradually being replaced by digital-type image input apparatuses. In most cases, the digital-type image input apparatuses optically read a subject to be photographed and photoelectrically convert the image into an electric signal, which is then converted into a digital signal. Subsequently, the image input apparatuses perform predetermined image processing on the digital image. The resulting image information is then output to an external source as digital information of a predetermined data format.

The above predetermined data formats include coding systems for performing high-efficiency coding on image information, such as MH, MR, MMR, TIFF, JPEG, and MPEG.

A reproducing apparatus decodes the coded digital information by using decoding algorithms corresponding to the coding system used in the image input apparatus. The

decoded information is then reproduced as the original image that can be viewed by humans through an output apparatus, such as a printer or a display unit.

The digital image information coded in the above-described predetermined data format will be simply referred to as "coded image information" hereinafter. It is, in general, very easy to incorporate the coded image information into an image processing apparatus, for example, a personal computer, and to edit the image information by using image information editing software.

According to the digital system, when the coded image information or the edited image information is copied, the image quality of the copied information is exactly the same as that of the original information. In contrast, the image quality of analog information is always degraded when copied. In view of maintaining image quality, the digital system is a significant improvement over the analog system.

In the analog system, however, the image quality of analog information is invariably degraded when copied. Accordingly, illegal copying does not present a serious practical problem.

On the other hand, in the digital system, it is possible to produce unlimited numbers of copies which are identical to the original. Accordingly, anyone is able to freely copy the original, i.e., consumers are able to copy a

product, such as a movie, without paying a royalty for the copied movie to the copyright holder, which inevitably becomes a major problem for copyright holders.

Alternatively, if the original of the coded image information is recorded on a computer, the following may occur. A cracker may illegally access the computer and copy the image information, which may be then sold at a cost lower than the legitimate product, or it may be reedited and sold as another product.

As an effective countermeasure against the aforementioned copying of digital information, an encrypting technique may be used. To "encrypt" is to convert the original information into a coded form that is not understood by anyone other than authorized users.

Generally, an encryption operation is performed by information processing apparatuses, such as computers. More specifically, the original image produced by an image input apparatus is temporarily stored in an information processing apparatus and is then encrypted. A decryption key for decoding the encrypted image is safely stored within the information processing apparatus.

Thus, even if the encrypted image information recorded on the image processing apparatus is illegally copied, the illegal user is unable to read the content of the encrypted image information unless the decryption key is obtained.

That is, by encrypting the original image in the information processing apparatus, the copyright of the image information can be safely protected.

As noted above, however, the original image produced in the image input apparatus is first output to the information processing apparatus and is then encrypted. If the image information is accessed during the period from which the image information is output from the image input apparatus to which it is encrypted in the information processing apparatus, such as a computer, there may be the danger of illegally copying the image information, thereby jeopardizing the security of the image information.

Additionally, a decryption key for decoding the encrypted image information, which is safely stored in the image information processing apparatus, may be illegally obtained by the users other than authorized users by using a new method of attack.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to solve the above-described problems.

It is another object of the present invention to provide an image input apparatus in which the privacy and the security of image information are enhanced and the copyright of the image information is protected more

reliably by assigning different encryption keys to a plurality of users without increasing the complexity of an encryption unit.

It is still another object of the present invention to provide an image input method in which the privacy and the security of image information are enhanced and the copyright of the image information is protected more reliably by assigning different encryption keys to a plurality of users without increasing the complexity of encryption processing.

It is a further object of the present invention to provide a recording medium in which the privacy and the security of image information are enhanced and the copyright of the image information is protected more reliably by assigning different encryption keys to a plurality of users.

It is a further object of the present invention to provide an encryption processing program stored in a computer-readable medium, in which the privacy and the security of image information are enhanced and the copyright of the image information is protected more reliably by assigning different encryption keys to a plurality of users without increasing the complexity of encryption processing.

To achieve the above objects, according to one aspect of the present invention, there is provided an image input apparatus including conversion means for converting an image signal into digital information. Encryption means encrypts

the digital information by using a first encryption key. Erasing means erases the first encryption key after the digital information has been encrypted.

According to another aspect of the present invention, there is provided an image input apparatus including conversion means for converting an image signal into digital information. Input means inputs an encryption key from an external source. Encryption means encrypts the digital information by using the encryption key.

According to still another aspect of the present invention, there is provided an image input apparatus including conversion means for converting an image signal into digital information. Information encrypting means encrypts the digital information by using an internal encryption key disposed within the image input apparatus. Input means inputs from an external source an external encryption key for encrypting the internal encryption key. Key encrypting means encrypts the internal encryption key by using the external encryption key.

According to a further aspect of the present invention, there is provided an image input method including the steps of: converting an image signal into digital information; encrypting the digital information by using an encryption key; and erasing the encryption key after the digital information has been encrypted.

According to a yet further aspect of the present invention, there is provided an image input method including the steps of: converting an image signal into digital information; inputting an encryption key from an external source; and encrypting the digital information by using the encryption key.

According to a further aspect of the present invention, there is provided an image input method including the steps of: converting an image signal into digital information; encrypting the digital information by using an internal encryption key disposed within the image input apparatus; obtaining from an external source an external encryption key for encrypting the internal encryption key; and encrypting the internal encryption key by using the external encryption key.

According to a further aspect of the present invention, there is provided a recording medium attachable to and detachable from an image processing apparatus for encrypting a digital image signal. The recording medium includes means for supplying to the image processing apparatus an encryption key required for encrypting the digital image signal. Recording means records a decryption key corresponding to the encryption key.

According to a further aspect of the present invention, there is provided a recording medium attachable to and

detachable from an image processing apparatus for encrypting a digital image signal by using a first encryption key and for encrypting the first encryption key by using a second encryption key. The recording medium includes means for supplying the second encryption key to the image processing apparatus. Recording means records a decryption key corresponding to the first encryption key.

According to a further aspect of the present invention, there is provided an encryption processing program stored in a computer-readable medium. The encryption processing program includes: a step of converting an image signal into digital information; a step of encrypting the digital information by using an encryption key; and a step of erasing the encryption key after the digital information has been encrypted.

According to a further aspect of the present invention, there is provided an encryption processing program stored in a computer-readable medium. The encryption processing program includes: a step of converting an image signal into digital information; a step of encrypting the digital information by using an internal encryption key disposed within the image input apparatus; a step of obtaining from an external source an external encryption key for encrypting the internal encryption key; and a step of encrypting the internal encryption key by using the external encryption key.

Still other objects of the present invention, and the advantages thereof, will become fully apparent from the following detailed description of the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating the configuration of an image input apparatus according to a first embodiment of the present invention;

Fig. 2 is a block diagram illustrating the configuration of an IC card;

Fig. 3 is a flow chart illustrating encryption processing according to the first embodiment of the present invention;

Fig. 4 is a block diagram illustrating the configuration of an image input apparatus according to a second embodiment of the present invention; and

Fig. 5 is a flow chart illustrating encryption processing according to the second embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of the present invention will now be described in detail hereinafter with reference to the accompanying drawings.

1. Encryption Technique

In encryption processing, original data is referred to as "plaintext". To convert the plaintext into a ciphertext that is meaningless to unauthorized users is referred to as "encryption", and the conversion procedures for an encryption operation are referred to as "encryption algorithms". The plaintext includes not only text data, but also all types of information data, such as sound data and image data.

"Encryption" is a conversion using a parameter, such as an encryption key. To obtain the plaintext from the ciphertext by an authorized user is referred to as "decrypting", which is performed by using a parameter corresponding to the encryption key, which is referred to as a "decryption key".

For an illegal user to recover the plaintext from the ciphertext by using any means or to illegally find the decryption key is referred to as "cryptanalysis". According to the modern cryptographic techniques, the security of cryptography relies on an encryption key or a decryption key. Thus, even if a user knows the encryption algorithm, the user is unable to obtain the plaintext unless the user has the key. As a result, even the programmer who has produced the encryption algorithm cannot succeed in the cryptanalysis.

Many types of encryption algorithms are currently

available, and they are broadly classified into two systems, such as asymmetric cryptosystems (public key cryptosystems) and symmetric cryptosystems (conventional cryptosystems), according to whether the encryption key may be publicly obtained.

In an asymmetric cryptosystem, i.e., a public key cryptosystem, an encryption key and a decryption key are different, and the decryption key cannot easily be calculated from the encryption key. The encryption key and the decryption key in this system are referred to as the "public key" and the "private key", respectively.

The asymmetric cryptosystem has the following features.

(1) The encryption key and the decryption key are different. It is not necessary to secretly deliver the encryption key, which can be available to the public, and it is easy to deliver the key.

(2) Since the user's encryption key is available to the public, the user needs to store only the user's own decryption key secretly.

(3) An authentication function can be provided to verify that identity of the sender of the transmitted message and that the message has not been tampered. As an asymmetric cryptosystem that can achieve both the encryption function and the authentication function, the RSA cipher system (R. L. Rivest, A. Schamir and L. Adleman, "A method

of obtaining digital signatures and public key cryptosystems", Comm of ACM,) is known. As one of the above type of asymmetric cryptosystems, the ElGamal cryptosystem (T. E. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transaction on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985) is well known.

As an asymmetric cryptosystem that can achieve only the authentication function, the Fiat-Shamir scheme (A. Fiat, A. Shamir, "How to prove yourself: practical solutions of identification and signature problems," Proc. of CRYPTO' 86, 1987) and the Schnorr scheme (C. P. Schnorr, "Emcient signature generation by smart cards," Journal of Cryptology vol. 4, pp. 161-174, 1991) are well known.

In a symmetric cryptosystem, on the other hand, which is also referred to as the "common key cryptosystem", the encryption key and the decryption key are the same. Since the advent of the public key cryptosystem in the latter half of 1970', the symmetric cryptosystem has also been referred to as the "conventional cryptosystem". The symmetric cryptosystems are classified into two types, i.e., block ciphers and stream ciphers. In the former, each character string (block) of a predetermined length is encrypted by the same key, and in the latter, the individual character strings or the individual bits are encrypted by using

different keys.

Block ciphers include transposition ciphers for encrypting a block by transposing the order of the character string, and substitution ciphers for encrypting a block by substituting a character with another character. For example, Data Encryption Standard (DES) and Fast data Encipherment ALgorithm (FEAL) are commercially available.

In stream ciphers, an exclusive-or (XOR) is performed on a message by using a random number, thereby disordering the content of the message. As this type of cipher, the Vernam cipher is well known in which a random number sequence is used as a one-time disposable key.

2. First Embodiment

Fig. 1 is a block diagram illustrating the configuration of an image input apparatus according to a first embodiment of the present invention. In Fig. 1, an image input apparatus 100 is formed of a tamper resistant module 10, a mechanical driving unit 6, an operation unit 8, and an external interface 7. An integrated circuit (IC) card 20 is attachable to and detachable from the image input apparatus 100. The IC card 20 is also attachable to and detachable from an image processing apparatus 200, which is separately disposed from the image input apparatus 100. The image processing apparatus 200 is, for example, a computer. By connecting the IC card 20 to the information processing

apparatus 200, the image information encrypted by an encryption key of the IC card 20 can be decrypted.

The tamper resistant module 10 integrates an image pick-up unit 1, a central information processing unit (hereinafter referred to as a "CPU") 2, a control program memory 3, a work memory 4, and an encryption unit 5.

In the tamper resistant module 10, upon detecting that the data processed by the encryption unit 5 is being physically removed, the CPU 2 is adapted to erase and destroy the program and data stored in the control program memory 3 and in the work memory 4.

In the image input apparatus 100 of this embodiment, the image pick-up unit 1 picks up an image of a subject to generate an analog image signal and further converts it to a digital image signal. The image pick-up unit 1 controls, based on the program stored in the control program memory 3, the signal processing executed on the digital image signal so that good visual images are obtained.

Subsequently, the CPU 2 performs a predetermined image processing on the digital image information and then performs high-efficiency coding on the image information. The coded image information is then supplied to the encryption unit 5. Thereafter, the encryption unit 5 encrypts the digital image information by using the encryption key input from the IC card 20 through the

external interface 7 and outputs the encrypted image information. The encrypted image information is then stored in a storage medium (not shown). The external interface 7 is used for receiving an encryption key from an external unit and for outputting encrypted information from the apparatus.

The tamper resistant module 10 is constructed in such a manner that the data and the content of communications stored within the image pick-up unit 1, the CPU 2, the control program memory 3, the work memory 4, and the encryption unit 5 are prevented from being output to an external source until the encryption processing is completed.

The cryptosystem and the method for setting the encryption key used for performing encryption in the first embodiment are described below. As noted above, there are two types of cryptosystems, such as the public key cryptosystem and the common key cryptosystem. In using the common key cryptosystem, it is necessary to specify that the encryption key (hereinafter referred to as the "common key") without being known to unauthorized users. If, on the other hand, the public key cryptosystem is used, it is not necessary to specify that the encryption key (hereinafter referred to as the "public key") without being known to unauthorized users since it can be available to the public.

There are the following three methods for setting the

encryption key. In the first method, the encryption key is stored in the control program memory 3 in advance when the image input apparatus 100 is manufactured. In the second method, the encryption key is input from the operation unit 8, and in the third method, the encryption key is input from the IC card 20 through the external interface 7.

In the first method, the different encryption keys may be stored in the individual apparatuses, or the same encryption key may be stored in all the apparatuses of a certain type. Whichever approach is employed, the decryption key corresponding to the encryption key should be known only to the authorized users for the apparatus. Accordingly, special attention is required. Moreover, it is difficult to assign the different encryption keys to a plurality of users, so that, in practice, it is necessary to share the same encryption key and decryption key for all the users.

In the second method, since the user of the apparatus can directly input the encryption key which is known only to the user, there is a small probability that the encryption key will be revealed to unauthorized users. Thus, the security can be enhanced over the first method. However, in such a complicated encryption processing having a high level of security, it is not always easy for humans to set the encryption key. Thus, if the size or the content of the

encryption key is too large or too difficult to store and input, the input operation becomes troublesome and a nuisance for the user.

In the third method, a suitable external apparatus, for example, the IC card 20, is connected to the external interface 7, and the encryption key is input into the image input apparatus 100 from the external apparatus. In this method, if communications for inputting the encryption key are automatically performed between the external apparatus and the image input apparatus 100 as required, the drawbacks of the first method can be overcome, and also, the time and effort required by users are lessened.

In the following description of the first embodiment, it is now assumed that the IC card 20 shown in Fig. 2 is used as the external apparatus to be connected to the external interface 7. The user of the image input apparatus 100 carries the IC card 20 in which a memory 23 having a certain storage capacity and a processing unit 24 having a calculation capacity are stored. It is now assumed that the encryption key and the corresponding decryption key which are known only to the user are stored in the IC card 20.

The IC card 20 is manufactured in such a manner that it is very difficult to obtain the encryption key even if the IC card 20 is disassembled. The user connects the IC card 20 to the external interface 7 when using the image input

apparatus 100. The image input apparatus 100 then encrypts the picked-up image with the encryption key input from the IC card 20 and outputs the encrypted image information. The encryption key input into the image input apparatus 100 is always erased after the image information has been encrypted.

Namely, by using the IC card 20, the encrypted image information can be decrypted only by the user who has the decryption key corresponding to the encryption key stored in the IC card 20. Accordingly, the user simply connects the IC card 20 to the external interface 7 before performing a photographic operation, and the picked-up encrypted image information can be obtained merely by performing a photographic operation. In the third method, therefore, the burden in inputting the encryption key can be significantly reduced compared to the second method.

As discussed above, by using the IC card 20, the image information can be encrypted by employing either of the public key cryptosystem or the common key cryptosystem. The image processing apparatus 200 is able to decrypt the encrypted image information with the decryption key stored in the IC card 20, thereby obtaining the high-efficiency coded image information.

The third method is discussed in detail below when the common key cryptosystem, for example, is used alone. The IC card 20 is used as the external apparatus, as illustrated in

Fig. 1. The IC card 20 shown in Fig. 2 includes an encryption key generator 25 for generating a common key and a communication unit 21 for inputting the common key into the image input apparatus 100.

The common key is produced by means such as generating a random number. The user connects the IC card 20 to the image input apparatus 100 via the external interface 7 and performs a photographic operation. The IC card 20 connected to the external interface 7 supplies the common key to the image input apparatus 100 via the communication unit 21.

The image input apparatus 100 encrypts the picked-up image with the common key by using the encryption unit 5, and then outputs the encrypted image information. The common key is erased from all the memory devices provided for the image input apparatus 100 after the encryption operation has been completed. Thereafter, the user connects the IC card 20 to the information processing apparatus 200, which is then able to decrypt the encrypted image information output from the image input apparatus 100 by using the common key read from the IC card 20.

As the above-described image input apparatus 100, a scanner, a digital still camera, or a digital video camera may be considered. A copying machine or a facsimile machine, both of which are provided with an image pick-up unit, may also be used.

Fig. 3 is a flow chart illustrating the encryption processing performed by the image input apparatus 100. In step S1, the image pick-up unit 1 of the image input apparatus 100 of the first embodiment optically picks up an image of a subject and generates an image signal.

In step S2, the image pick-up unit 1 then converts the image signal into digital information. Subsequently, in step S3, the CPU 2 performs high-efficiency coding on the digital information.

In step S4, the encryption key (the public key or the common key) for encrypting the coded digital information is read from the IC card 20 and is then set. Thereafter, in step S5, the encryption unit 5 encrypts the coded digital information with the encryption key set by the CPU 2. In step S6, the CPU 2 then erases the encryption key from all the memory devices, including the control program memory 3 and the work memory 4, from the image input apparatus 100 after the digital information has been encrypted.

According to the foregoing description, in the image input apparatus 100 constructed in accordance with the first embodiment of the present invention, the encryption key (the common key or the public key) required for the encryption operation is input from the external apparatus, i.e., the IC card 20, and is reliably erased after the encryption operation has been completed. This makes it possible to

protect the encryption key from being obtained by illegal users and also to enhance the user's convenience. The decryption key for decrypting the encrypted information is stored in the IC card 20 rather than being input into the image input apparatus 100, thereby also protecting the decryption key from being obtained by illegal users from the image input apparatus 100.

In the image input apparatus 100, upon detecting that any physical operation is being performed on the tamper resistant module 10, the program and the data required for encrypting information are removed and destroyed. It is thus possible to enhance the privacy and the security of the image information and also to protect the copyright of the image information more reliably.

In the image input apparatus 100, after the digitized image information has undergone high-efficiency coding, the coded image information is encrypted before being output to an external source. Accordingly, the image information output to the image processing apparatus 200 from the image input apparatus 100 is positively encrypted. Therefore, the copyright of the digital image information can be protected more reliably, thereby preventing illegal copying, use, viewing, sale, etc., of the image information.

Additionally, in the image input apparatus 100, since the encryption key for encrypting the digital image

information is input into the image input apparatus 100 from an external source, different encryption keys can be assigned to a plurality of users without increasing the complexity of the configuration of the image input apparatus 100. As a consequence, even if the single image input apparatus 100 is shared among a plurality of users, the privacy and the security of the image information between the users can be maintained, thereby more reliably protecting the copyrights of the image information picked up by the individual users.

3. Second Embodiment

In the first embodiment, the image input apparatus 100 that encrypts digital information by using the public key cryptosystem or the common key cryptosystem has been discussed.

In the second embodiment, an image input apparatus 400 that encrypts digital information by using a combination of the public key cryptosystem and the common key cryptosystem is described below.

In the second embodiment, as well as in the first embodiment, an IC card 20 is used as an attachable and detachable external apparatus for supplying an encryption key. The IC card 20 has, as illustrated in Fig. 2, the encryption key generator 25 for generating an encryption key, i.e., a public key, used in the public key cryptosystem.

The IC card 20 also has a communication unit 21 for supplying the public key to the image input apparatus 400. The image input apparatus 400 of the second embodiment includes an encryption key generator 409 for generating a common key by using a random number and an encryption unit 409 for performing encryption operations by using the public key or the common key.

The configuration of the image input apparatus 400 of the second embodiment is described below with reference to Fig. 4.

The image input apparatus 400 is formed, as shown in Fig. 4, of an image pick-up portion 401, a digital converter 402, a CPU 403 including a high-efficiency coding circuit, an encryption unit 404, an encryption key erasing unit 405, a communication unit 407, a recording unit 408, and an encryption key generator 409.

The image pick-up portion 401 picks up an image of a subject and generates an image signal. The digital converter 402 converts the image signal into digital information. The CPU 403 performs high-efficiency coding on the digital information and also controls the operations of the individual elements of the image input apparatus 400. The encryption unit 404 includes an encryption circuit for encrypting the coded digital information according to the common key cryptosystem. The encryption unit 404 also

contains an encryption circuit for encrypting the common key according to the public key cryptosystem.

The encryption key generator 409 generates a common key required for the encryption operation of the encryption unit 404. The encryption key erasing unit 405 erases all the encryption keys (the public key and the common key) after the encryption unit 404 has encrypted the digital information.

The communication unit 407 outputs the encrypted digital information and the encrypted common key to an external source. The recording unit 408 records the encrypted digital information on a recording medium.

The information processing apparatus 200 of the second embodiment is connectable to the above-described IC card 20. By connecting the IC card 20 to the information processing apparatus 200, the information processing apparatus 200 decrypts the encrypted common key by using the decryption key read from the IC card 20, and then decrypts the encrypted image information with the common key decrypted.

A description is given hereinbelow of the encryption processing performed by the image input apparatus 400 constructed as described above.

The user performs a photographic operation by connecting the IC card 20 to the image input apparatus 400. In this case, the IC card 20 supplies the public key to the

image input apparatus 400.

Referring to Fig. 5, in step S51, in response to the user's operation, the image pick-up portion 401 of the image input apparatus 400 optically picks up an image of a subject and generates an image signal. In step S52, the digital converter 402 then converts the image signal into digital information. Subsequently, in step S53, the CPU 403 performs high-efficiency coding on the digital information by using the high-efficiency coding circuit.

In step S54, the encryption key generator 409 of the image input apparatus 400 generates a common key by using a random-number generating circuit, and the encryption unit 404 encrypts the coded digital information with the generated common key. Simultaneously, in step S55, the common key is further encrypted in the encryption unit 404 by using the public key input from the external IC card 20. Thereafter, in step S56, the common key and the public key are erased from all the memory devices of the image input apparatus 400 after the digital information has been encrypted.

As discussed above, according to the image input apparatus 400 constructed in accordance with the second embodiment of the present invention, it is performed by a combination of the public key input from an external apparatus, i.e., the IC card 20, and the common key

generated by the image input apparatus 400. Thus, the privacy and the security of the image information can be enhanced to a higher level, and any copyright of the image information can be protected more reliably.

In the image input apparatus 400, after the digital image information is encrypted and the encryption key is encrypted by another encryption key, each encryption key according to the respective cryptosystems is completely erased, thereby preventing each encryption key from being obtained by illegal users. The decryption key for decrypting the encrypted digital information is retained in the external IC card 20 rather than residing in the image input apparatus 400, thereby also protecting the decryption key from being obtained from the image input apparatus 400 by illegal users.

In the image input apparatus 400, after the digitized image information has undergone high-efficiency coding, the coded image information is encrypted before being output to an external source. Accordingly, the image information output to the image processing apparatus 200 from the image input apparatus 400 is positively encrypted. Therefore, the copyright of the digital image information can be protected more reliably, and illegal copying, use, viewing, sale, etc., of the image information can be prevented.

Additionally, in the image input apparatus 400, since

the encryption key for encrypting the digital image information is encrypted by another encryption key stored in the IC card 20, different encryption keys can be assigned to a plurality of users without increasing the complexity of the configuration of the image input apparatus 400. As a consequence, even if the single image input apparatus 400 is shared among a plurality of users, the privacy and the security of the image information among the users can be maintained, thereby more reliably protecting the copyrights of the image information picked up by individual users.

The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof.

For example, the image input apparatus 100 may be configured in the following manner to achieve the functions of the first embodiment. A software program code that implements the encryption function described in the first embodiment may be stored in the control program memory 3 shown in Fig. 1, and the CPU 2 shown in Fig. 1 may control the operation of the individual processing units of the image input apparatus 100 in accordance with the program code.

Similarly, the image input apparatus 400 may be configured in the following manner to attain the functions of the second embodiment. A software program code that

implements the encryption functions discussed in the second embodiment may be stored in the recording unit 408 shown in Fig. 4, and the CPU 403 shown in Fig. 4 may control the operations of the individual processing units of the image input apparatus 400.

As a storage medium for storing the above-described program code, a floppy disk, a compact disc-read only memory (CD-ROM), a magnetic tape, a hard disk, an optical disc, a magneto-optical disk, or a non-volatile memory card may be used.

Therefore, the above-mentioned embodiments are merely examples in all respects and must not be construed to limit the invention.

The scope of the present invention is defined by the scope of the appended claims, and is not limited at all by the specific descriptions of this specification. Furthermore, all the modifications and changes belonging to equivalents of the claims are considered to fall within the scope of the present invention.

WHAT IS CLAIMED IS:

1. An image input apparatus comprising:

conversion means for converting an image signal into digital information;

encryption means for encrypting the digital information by using an encryption key; and

erasing means for erasing said encryption key after the digital information has been encrypted.

2. An image input apparatus according to claim 1, wherein said encryption means encrypts the digital information which has undergone a high-efficiency coding operation.

3. An image input apparatus according to claim 1, further comprising image pick-up means for optically picking up an image of a subject and for generating an image signal from the picked-up image.

4. An image input apparatus according to claim 1, further comprising means for inputting said encryption key from an external source.

5. An image input apparatus according to claim 1,

further comprising means for generating said encryption key within said image input apparatus.

6. An image input apparatus according to claim 1, wherein said encryption key comprises an encryption key based on a common key cryptosystem.

7. An image input apparatus according to claim 1, wherein said encryption key comprises an encryption key based on a public key cryptosystem.

8. An image input apparatus according to claim 1, further comprising means for inputting from an external source another encryption key for encrypting said encryption key.

9. An image input apparatus according to claim 8, wherein said encryption key comprises an encryption key based on a common key cryptosystem, and said other encryption key comprises an encryption key based on a public key cryptosystem.

10. An image input method comprising the steps of:

converting an image signal into digital information;

encrypting the digital information by using an

encryption key; and

erasing said encryption key after the digital information has been encrypted.

11. An image input method according to claim 10, wherein the digital information which has undergone a high-efficiency coding operation is encrypted.

12. An image input method according to claim 10, wherein the image signal generated from an optically picked up image of a subject is converted into the digital information.

13. An image input method according to claim 10, wherein said encryption key comprises an encryption key based on one of a common key cryptosystem and a public key cryptosystem.

14. An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of encrypting the digital information by using an encryption key; and

a step of erasing said encryption key after the digital

information has been encrypted.

15. An image input apparatus comprising:

conversion means for converting an image signal into digital information;

means for inputting an encryption key from an external source; and

encryption means for encrypting the digital information by using said encryption key.

16. An image input method comprising the steps of:

converting an image signal into digital information;

inputting an encryption key from an external source; and

encrypting the digital information by using said encryption key.

17. A recording medium attachable to and detachable from an image processing apparatus for encrypting a digital image signal, said recording medium comprising:

means for supplying to said image processing apparatus an encryption key required for encrypting the digital image signal; and

means for recording a decryption key corresponding to said encryption key.

18. An image input apparatus comprising:

conversion means for converting an image signal into digital information;

information encryption means for encrypting the digital information by using an internal encryption key disposed within said image input apparatus;

means for inputting from an external source an external encryption key for encrypting said internal encryption key; and

key encryption means for encrypting said internal encryption key by using said external encryption key.

19. An image input apparatus according to claim 18, wherein said internal encryption key comprises an encryption key based on a common key cryptosystem, and said external encryption key comprises an encryption key based on a public key cryptosystem.

20. An image input method comprising the steps of:

converting an image signal into digital information;

encrypting the digital information by using an internal encryption key disposed within said image input apparatus;

obtaining from an external source an external encryption key for encrypting said internal encryption key;

and

encrypting said internal encryption key by using said external encryption key.

21. A recording medium attachable to and detachable from an image processing apparatus for encrypting a digital image signal by using a first encryption key, and for encrypting said first encryption key by using a second encryption key, said recording medium comprising:

means for supplying said second encryption key to said image processing apparatus; and

means for recording a decryption key corresponding to said first encryption key.

22. An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of encrypting the digital information by using an internal encryption key disposed within said image input apparatus;

a step of obtaining from an external source an external encryption key for encrypting said internal encryption key; and

a step of encrypting said internal encryption key by

using said external encryption key.

ABSTRACT OF THE DISCLOSURE

In an image input apparatus provided with an image pick-up unit, an image signal generated by the image pick-up unit is converted into digital information. The digital information is then encrypted by using an encryption key. The encryption key is input into the image input apparatus from an external apparatus, such as an IC card. The image input apparatus erases the encryption key after the digital information has been encrypted. With this arrangement, unauthorized users can be prevented from obtaining the encryption key, and different encryption keys can be assigned to a plurality of users. Thus, the privacy and the security of the image information can be enhanced, and the copyright of the image information can be protected more reliably.

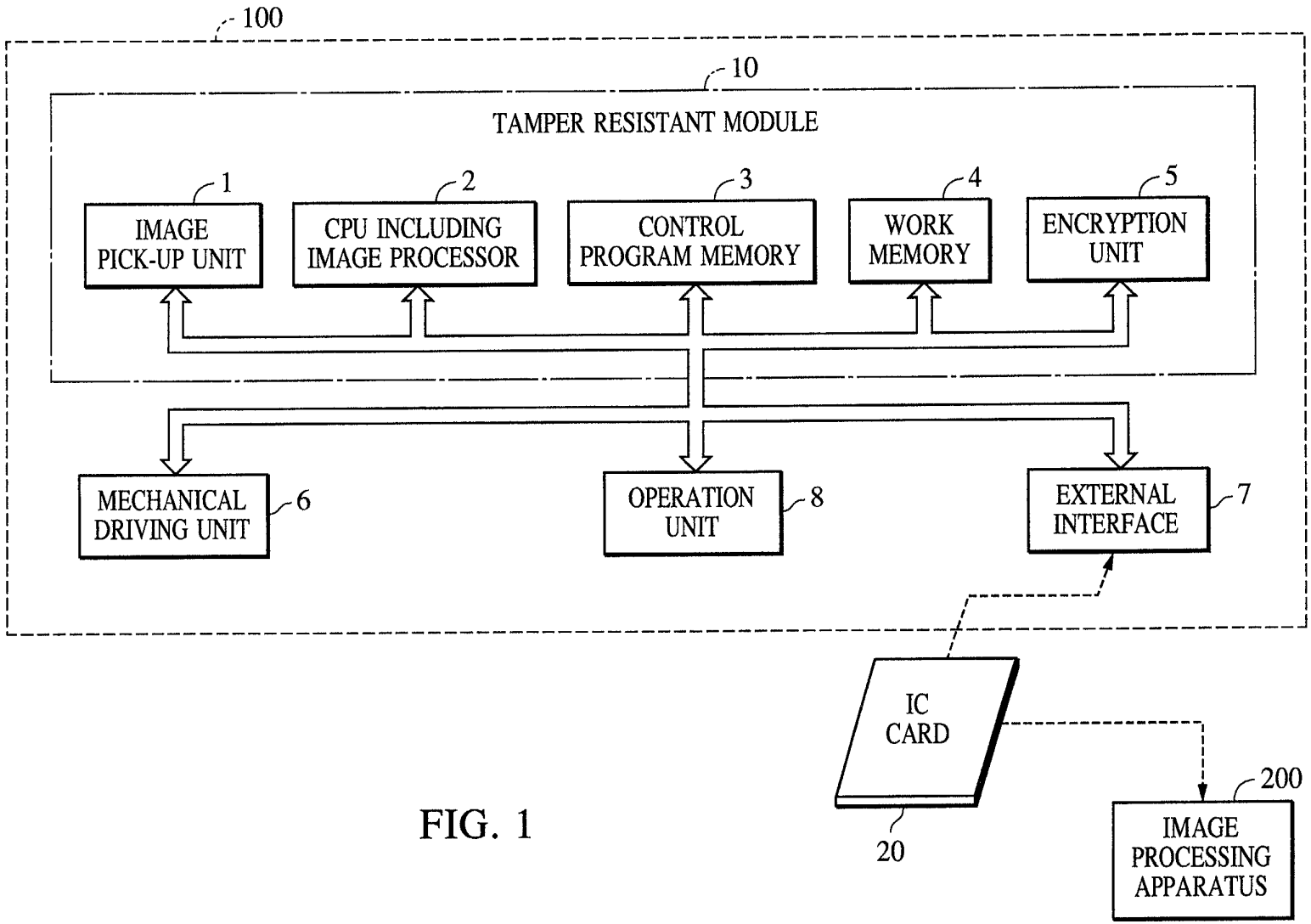


FIG. 1

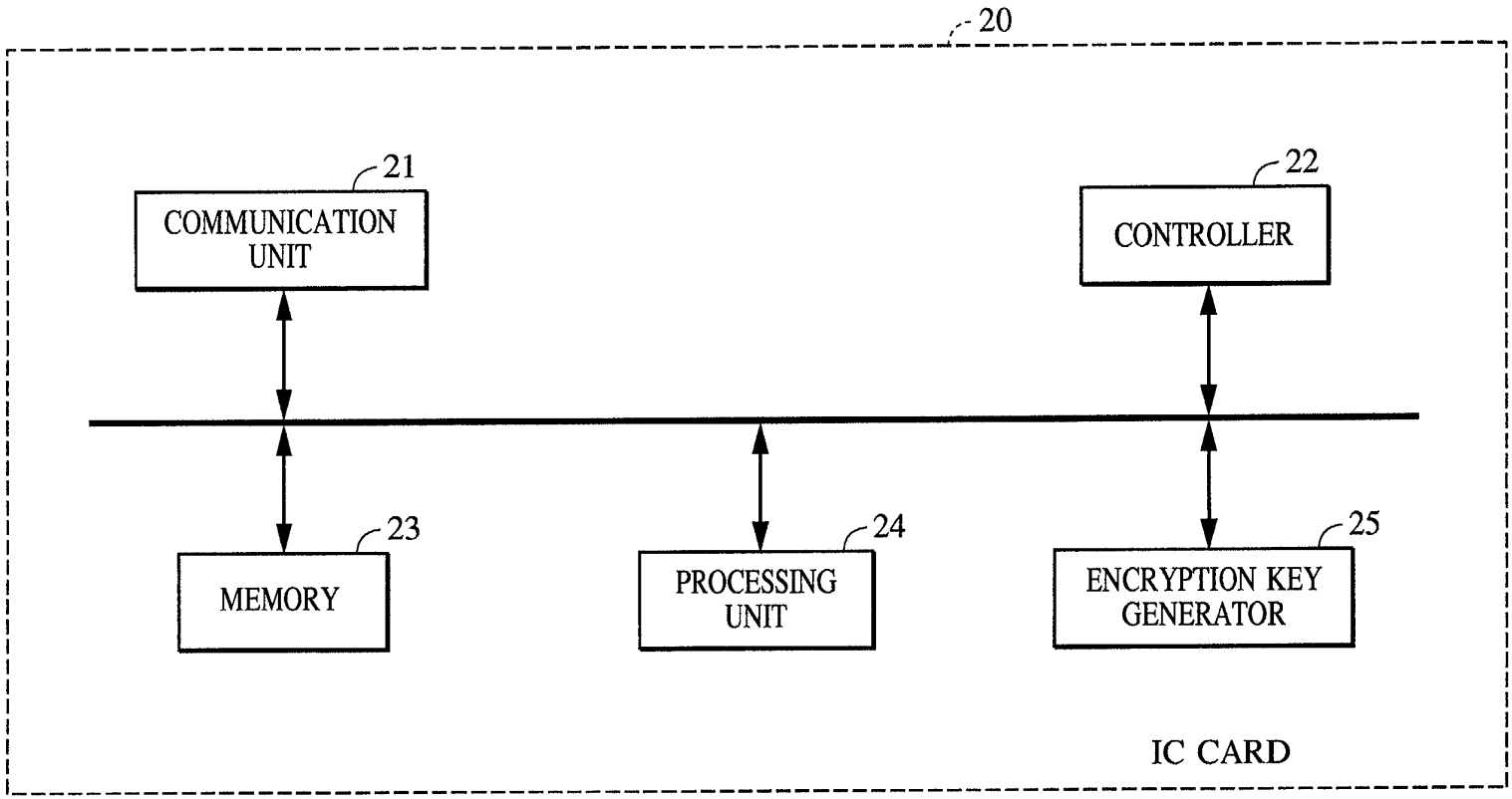

20
21
COMMUNICATION UNIT
22
CONTROLLER
23
MEMORY
24
PROCESSING UNIT
25
ENCRYPTION KEY GENERATOR
IC CARD

FIG. 2

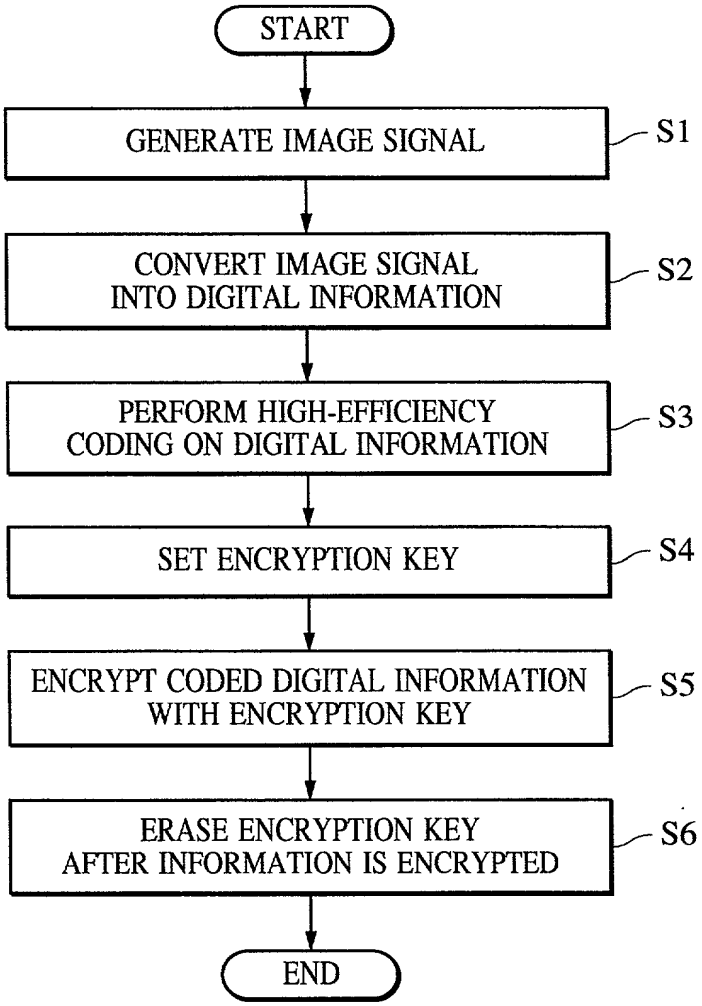

START
GENERATE IMAGE SIGNAL
S1
CONVERT IMAGE SIGNAL INTO DIGITAL INFORMATION
S2
PERFORM HIGH-EFFICIENCY CODING ON DIGITAL INFORMATION
S3
SET ENCRYPTION KEY
S4
ENCRYPT CODED DIGITAL INFORMATION WITH ENCRYPTION KEY
S5
ERASE ENCRYPTION KEY AFTER INFORMATION IS ENCRYPTED
S6
END

FIG. 3

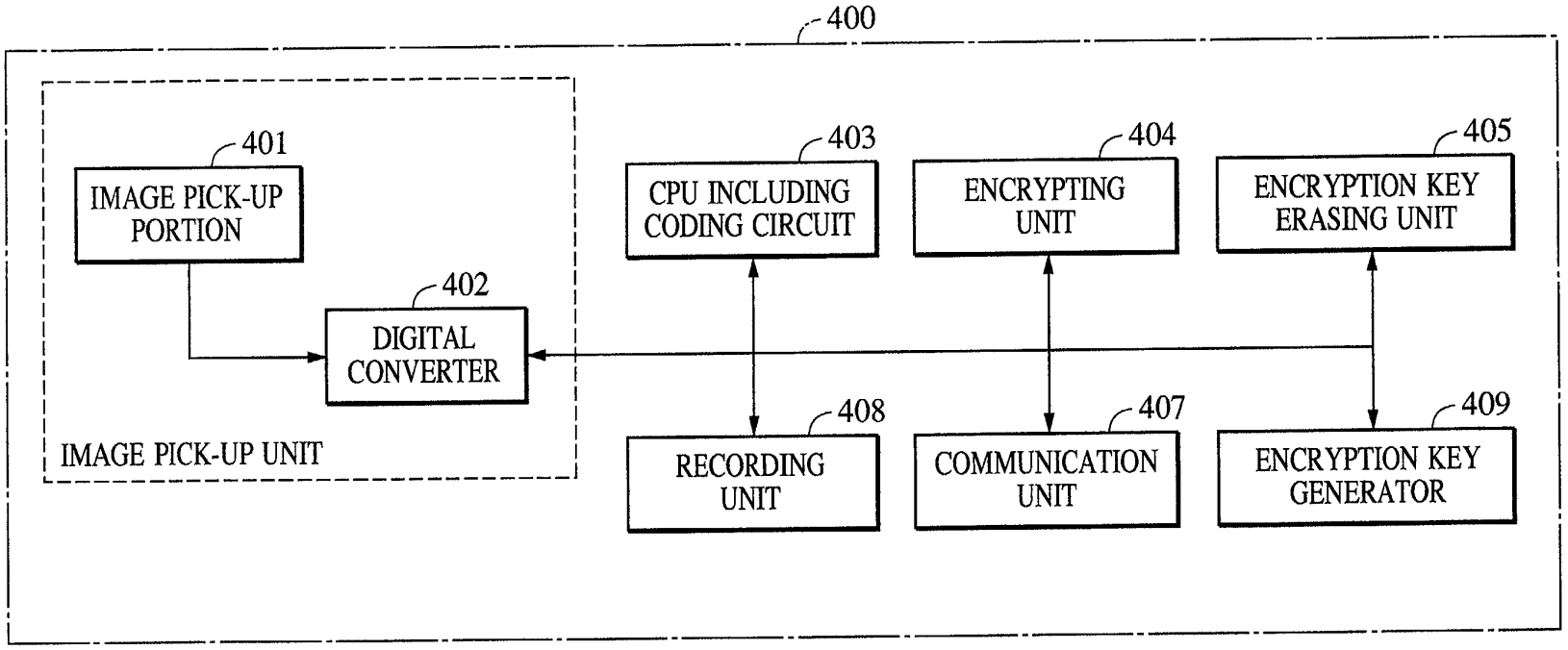

400
401
IMAGE PICK-UP PORTION
402
DIGITAL CONVERTER
IMAGE PICK-UP UNIT
403
CPU INCLUDING CODING CIRCUIT
404
ENCRYPTING UNIT
405
ENCRYPTION KEY ERASING UNIT
408
RECORDING UNIT
407
COMMUNICATION UNIT
409
ENCRYPTION KEY GENERATOR

FIG. 4

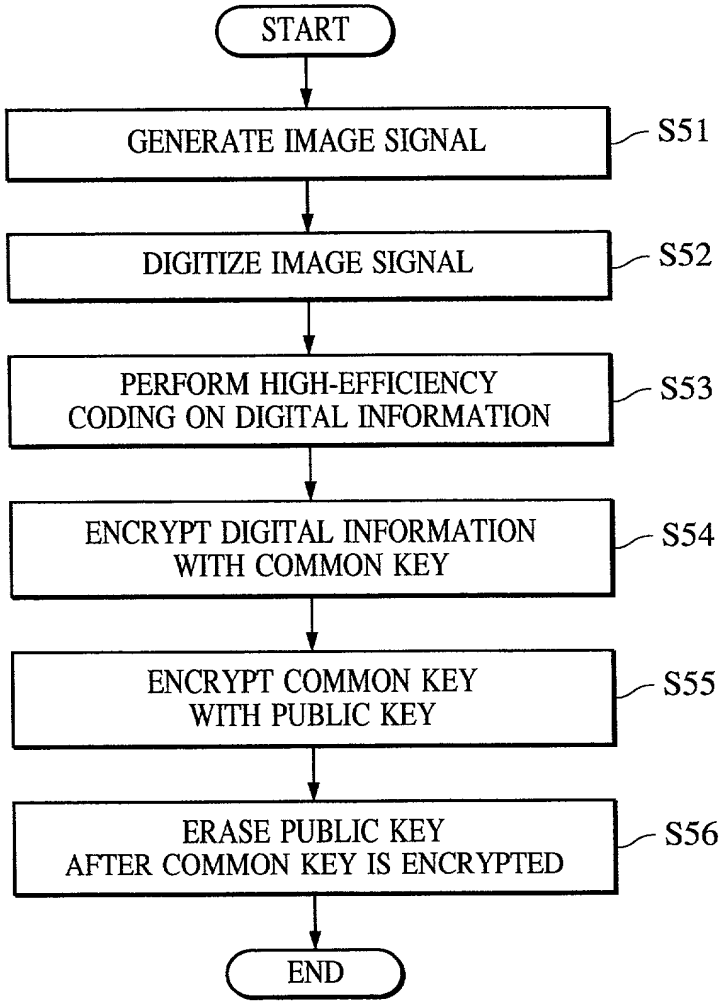

START
GENERATE IMAGE SIGNAL
S51
DIGITIZE IMAGE SIGNAL
S52
PERFORM HIGH-EFFICIENCY CODING ON DIGITAL INFORMATION
S53
ENCRYPT DIGITAL INFORMATION WITH COMMON KEY
S54
ENCRYPT COMMON KEY WITH PUBLIC KEY
S55
ERASE PUBLIC KEY AFTER COMMON KEY IS ENCRYPTED
S56
END

FIG. 5

COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
(Page 1)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled IMAGE INPUT APPARATUS, IMAGE INPUT METHOD, RECORDING MEDIUM, AND ENCRYPTION PROCESSING PROGRAM STORED IN COMPUTER-READABLE MEDIUM,

the specification of which [X] is attached hereto [ ] was filed on _____ as United States Application No. or PCT International Application No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b), of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designates at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT international application having a filing date before that of the application on which priority is claimed:

Country	Application No.	Filed (Day/Mo./Yr.)	(Yes/No) Priority Claimed
Japan	003367/1998 (Pat.)	January 9, 1998	Yes

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application No.	Filed (Day/Mo./Yr.)	Status (Patented, Pending, Abandoned)
N/A		

I hereby appoint the practitioners associated with the firm and Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to the address associated with that Customer Number.

FITZPATRICK, CELLA, HARPER & SCINTO
Customer Number: 05514

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor KAZUOMI OISHI

Inventor's signature _____

Date _____ Citizen/Subject of Japan

Residence 910 Camino Pescadero #27, Goleta, California 93117, USA

Post Office Address _____